THORLEY
WEALTH MANAGEMENT
Trust. Experience. Performance.
www.thorleywm.com

You've Been Hacked or Spoofed: Now What?

Unfortunately, many of us who become victim to any sort of information security breach won't know until someone else tells us. For example, we might get a message or call from a friend asking why we sent that "spammy" email with a link to a free Amazon gift card. Have we been hacked? Spoofed? And how do we prevent it from happening again?

Here, we'll discuss the difference between hacking and spoofing, plus provide some simple tips to help protect your personal information.

Spoofing Vs. Hacking

Let's start by taking a look at what happens when you've been spoofed versus what it means to be hacked.

Spoofing. You might think of spoofing as something like falsifying a letter sent via the USPS. Anyone can write a letter, sign someone else's name, and put that individual's return address on the envelope. If you were to receive that phony letter, you would likely believe that it came from the individual who supposedly signed it and from the return address indicated. In reality, it could have been sent from anyone, anywhere.

Spoofers often forge the header information of the emails they send (i.e., the To, From, and Subject lines, as well as the time stamp and path that the emails took to arrive in your inbox). They do this in an attempt to make it appear as if their messages came from someone or somewhere you know (e.g., a friend or familiar organization like Bank of America). The goal? To get you to respond to their spam or to click on the malware-laden links or attachments in their phony messages.

When an email address has been spoofed, the spammer doesn't gain access to your email account. Hacking, however, is a different story.

Hacking. This is when a criminal *actually gets into your email account*. He or she can do this in a number of ways—by sniffing your activity on a public Wi-Fi network, through a phishing email, or via password-guessing software. Once in, the hacker will have access to all the information stored in your email account. This might include your contact list, bank account numbers, credit card information, online transaction receipts, and emails from other organizations confirming changed passwords (making it easier to identify other accounts of yours that can be hacked).

What's Next?

Unfortunately, there is no way to prevent spoofing. If your email address can be viewed publicly somewhere on the internet, someone can spoof it. But there are steps that you can take if you've been hacked that will also help mitigate the risk of any future hacking attempts.

1478 Marsh Road
Pittsford, NY 14534
P: (585) 512-8453
F: (585) 625-0477
www.thorleywm.com

Change your password. Here, you will want to include any passwords for other accounts that are the same or similar to the compromised password. In creating new passwords, avoid using dictionary words or anything personally identifiable (e.g., your birth date). Also, be sure that your passwords are *at least* eight characters long and include upper- and lowercase letters, numbers, and special characters.

Modify the answers to your security questions. Either make up answers to the questions or add an extra letter or symbol to the real answers. That way, even if the hacker figures out the answers, he or she will still have a hard time accessing your accounts. For example, instead of answering "Jones" to the "What's your mother's maiden name?" question, add another symbol or character and make it "@Jones" or "JonesM."

Set up multifactor authentication. This feature requires you to provide more than a username and password to access your account. For example, an additional layer of authentication could be a passcode sent to your smartphone that you need to input when you log in.

Review your email account settings. The hacker may have altered your account settings so that copies of received emails will be automatically forwarded to his or her account. So, even after you resecure your email account, the hacker can keep tabs on you. He or she could also have placed fraudulent links in your email signature and automatic replies. Be sure to check your settings and verify that these were not altered.

Run a virus scan. It's also possible that the hacker inserted malware into your system through your email account. This could enable him or her to conduct *recon*—meaning that all of your online activity would be automatically reported back to the hacker and allow him or her to collect even more of your personal information.

Ensure that there was no financial or personally identifiable information in your email account. If personal information was stored, such as your social security number (SSN), date of birth, or account numbers, *strongly consider* getting the compromised account numbers changed. In addition, have the banks or other organizations report the new numbers to you over the phone, *not via email*. Also consider credit monitoring, especially if all or part of your SSN was compromised.

Protect Yourself!

To protect your personal information, be wary about connecting to public Wi-Fi networks and what you transmit over such networks, as this is one of the most common ways that cybercriminals obtain email addresses and passwords. In addition, be suspicious of unsolicited or spam emails. If you receive one from someone you know, let that individual know that his or her email may have been spoofed or hacked. By keeping these guidelines in mind, as well as the tips discussed here, you will be well positioned to keep your confidential information secure.

###